THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF UTAH

IN THE MATTER OF THE SEARCH OF:	)
	)
SEE ATTACHMENT A	)

Case No. 2:24mj995-DAO

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Curtis Cox ("Your Affiant"), a Special Agent (SA) with the Federal Bureau of Investigation (FBI), Salt Lake City Division, being duly sworn, depose and state as follows to wit:

1. I am employed as a Special Agent of the FBI and have been since April 2015. I am currently assigned to the Salt Lake City Field Office and am a member of the FBI Child Exploitation and Human Trafficking Task Force (CEHTTF). As a result of my training and experience, I am familiar with information technology and its use in criminal activities. Since joining the FBI, I have investigated violations of federal law and am currently investigating federal violations concerning child sexual abuse material (CSAM) and the sexual exploitation of children.

2. As a federal agent, I am authorized to investigate violations of laws of the United States and am a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

PURPOSE OF THE AFFIDAVIT

3. I make this affidavit in support of an application for a search warrant for the residence of JACOB HARE, described in Attachment A (the "SUBJECT PROPERTY"), for the items described in Attachment B hereto, which are the evidence, fruits, and instrumentalities of

the violations of 18 U.S.C. §§ 2252(a)(4), 2252A(a)(2), and (5)(B) (Receipt, Possession, and Access to View Child Pornography) (the "SUBJECT OFFENSES").

4. The statements in this Affidavit are based in part on information provided by law enforcement officers assigned to other law enforcement agencies, other Special Agents and employees of the FBI, and on my experience and background as a Special Agent of the FBI. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause for the requested search warrant.

BRIEF SUMMARY

5. As set forth in detail below, HARE was arrested on September 27, 2024, for attempted rape of a child, attempted sodomy on a child, and attempted human trafficking of a child. He lived at the SUBJECT PROPERTY until the time of his arrest. HARE is currently incarcerated at the Salt Lake County Jail. In September 2024, Hare made arrangements with a person whom he believed to be a 33-year-old male (father) to engage in sexual acts with the father's 10-year-old female child (daughter) for a cost of $250 cash. HARE arranged to arrive at a specified location in West Valley City, Utah, at a hotel and pay $250 cash for vaginal sex and oral sex with the 10-year-old female child. HARE was arrested after arriving at the pre-arranged meeting location. He was subsequently transported to the West Valley City Police Department and, after waiving his right to silence and counsel, interviewed. During the interview, HARE advised he has watched CSAM for approximately 20 years. HARE advised that he has watched CSAM using a computer device at his residence (SUBJECT PROPERTY). HARE confirmed

the computer device was still located at his residence and confirmed his residence to be the SUBJECT PROPERTY. There is therefore probable cause to believe that evidence of the SUBJECT OFFENSES will be found at HARE'S residence as described in Attachment A.

PROBABLE CAUSE

6. Based on my personal knowledge and experience, as well as information received from other individuals, including law enforcement officers, as well as their reports, as set forth below, I know the following:

7. On September 27, 2024, a law enforcement officer was working in an undercover capacity as part of the State Bureau of Investigation – State Child Exploitation Team during a joint operation with the CEHTTF. An individual, later identified as HARE, made contact with the undercover officer on a chat website. The undercover officer advised HARE that he was a 33-year -old male that was selling his 10-year-old female child to individuals who were willing to pay to perform sexual acts with the child. HARE arranged with a person whom he believed to be the father to meet with the father and child at a hotel in West Valley City. HARE made arrangements to pay $250 cash to have vaginal sex and oral sex with the 10-year-old female child. Members of the CEHTTF and other law enforcement officers established surveillance at the hotel and observed HARE arrive at the meeting location precisely at the time agreed upon in the chat. HARE was safely taken into custody. At the time of the arrest, $250 was located in HARE'S possession. In addition, HARE was wearing a "make-shift cock ring" to assist HARE in achieving an erection, in preparation to have sexual intercourse the child.

8. HARE was interviewed after he was read his *Miranda* Rights. HARE advised that he understood his rights and was willing to talk to investigators. HARE advised he was the

individual chatting with the person he believed to the 33-year-old father and that he made arrangements to meet with the father to have vaginal and oral sex with the 10-year-old female child for the agreed upon price of $250 cash.

9. During the interview, HARE advised he has regularly accessed and viewed CSAM for approximately 20 years. HARE advised that he uses a laptop/tablet/computer device which is located at his residence (the SUBJECT PROPERTY) to access and view CSAM. HARE confirmed he has lived at the same address almost his entire life. HARE'S Residence is located at 6373 S Cyclamen Way West Jordan, Utah (the SUBJECT PROPERTY). HARE confirmed the laptop/tablet/computer device was still at the SUBJECT PROPERTY. HARE disclosed to the interviewing Agents that he has viewed CSAM that depicted adults performing sexual acts with toddlers while HARE masturbated.

10. Based on the totality of the circumstances described above, it appears that HARE is someone with a sexual interest in children and images of children. HARE arranged, and traveled to, a meeting with a person he believed to be offering his ten-year-old daughter for sex. HARE brought the agreed-upon sum of money and prepared for sexual intercourse with the minor girl by applying and wearing a "cock ring." Following his arrest, HARE acknowledged accessing and viewing CSAM that depicted children as young as toddlers being sexually abused by adults while HARE sexually pleasured himself. Based upon my knowledge, experience, and training in CSAM investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals who, like HARE, have a sexual interest in children and images of children:

a. The majority of individuals who, like HARE, possess sexualized images of children

and CSAM are persons who have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.

b. Individuals who possess sexualized images of children and CSAM often collect sexually explicit materials of children.

c. These individuals often also collect child erotica, which may consist of images or text that do not rise to the level of CSAM, but which nonetheless fuel their deviant sexual fantasies involving children. Non-pornographic, seemingly innocuous images of minors, are often found on computers and digital storage devices that also contain CSAM, or that is used to communicate with others about sexual activity or interest in children. Such images are useful in attempting to identify actual minors depicted in CSAM images found during the execution of a search warrant. In certain cases, such images may also assist in determining the origins of a particular CSAM image or series of images. These materials also evidence a sexual interest in children, which is evidence related to knowledge, motive, and intent regarding CSAM images an individual may also possess.

d. In the past, it was common for these materials (CSAM and child erotica) to be stored in hard copies such as photographs, magazines, and books. As digital technology has evolved, it is more common for such individuals to store this material digitally – either on digital devices such as phones, thumb drives, or computers, or stored in the cloud but easily accessible via devices such as phones or computers. As Internet download speeds get faster, it is also common for

individuals to use their devices to access and view images online, without downloading or saving them. This allows them to delete their collection of CSAM, as well as wipe their digital devices, in an attempt to destroy evidence and evade law enforcement, while still maintaining access to images whenever they are connected to the internet.

e. Regardless of how the material is stored, such individuals tend to value this material and do not like to be without access to it for long periods of time. They regularly maintain their collections or the devices that give them access to this material in the privacy and security of their homes, cars, garages, sheds, or other secure storage location, such as on their person. As discussed above, there is probable cause to believe that HARE has CSAM on digital devices at his home, the SUBJECT PROPERTY.

11. Even in the unlikely event that HARE has deleted the CSAM he acknowledged accessing and viewing, evidence that such material was on the devices can often be found through the use of computer forensics. Evidence can be found months, even years, later.

12. Based on the information set forth above, there is probable cause to believe that evidence of the SUBJECT OFFENSES will be found at the SUBJECT PREMISES.

DEFINITIONS

13. The following definitions apply to this Affidavit and Attachment B to this Affidavit:

14. "Child Pornography" includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

15. "Visual depictions" includes prints, copies of visual images, developed and undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

16. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

17. "IP Address" means Internet Protocol address, which is a unique numeric address used by computers on the Internet. Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

18. "Internet" means a global network of computers and other electronic devices that

communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

19. In this affidavit, the terms "computers" or "digital storage media" or "digital storage devices" may be used interchangeably, and are intended to include any physical object upon which computer data can be recorded as well as all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices capable of performing logical, arithmetic, or storage functions, including desktop and laptop computers, mobile phones, tablets, server computers, game consoles, network hardware, hard disk drives, RAM, floppy disks, flash memory, CDs, DVDs, and other magnetic or optical storage media.

SEIZURE AND SEARCH OF COMPUTERS

20. As described above and in Attachment B, I submit that if computers or storage media are found at the SUBJECT PRESMISES, there is probable cause to search and seize those items for the reasons stated below. Some of these electronic records might take the form of files, documents, and other data that is user-generated. Some of these electronic records, as explained below, might take a form that becomes meaningful only upon forensic analysis. They may be seized and searched on-scene, and/or searched off-scene in a controlled environment.

21. For example, based on my knowledge, training, and experience, I know that a powered-on computer maintains volatile data. Volatile data can be defined as active information temporarily reflecting a computer's current state including registers, caches, physical and virtual memory, network connections, network shares, running processes, disks (floppy, tape and/or CD-ROM), and printing activity. Collected volatile data may contain such information as

opened files, connections to other computers, passwords used for encryption, the presence of anti-forensic tools, or the presence of programs loaded in memory that would otherwise go unnoticed. Volatile data and its corresponding evidentiary value is lost when a computer is powered-off and unplugged.

22. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

23. Also, again based on my training and experience, wholly apart from user-generated files, computer storage media contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, virtual memory "swap" or paging files, and shadow copies of previous versions of systems or files, or paging files. Computer users typically do not erase or delete this evidence because special software is typically required for that task. However, it is technically

possible to delete this information. Data on the storage medium not currently associated with any file can provide evidence of a file that was once on the storage medium but has since been deleted, edited, moved, or show a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

24. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for evidence that establishes how computers were used, why they were used, the purpose of their use, and the purposes to which they were put, who used them, the state of mind of the user(s), and when they were used.

25. The monitor and printer are also essential to show the nature and quality of the images or files that the system can produce. In addition, the analyst needs all assisting software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instructional manuals or other documentation and security devices. Moreover, searching computerized information for evidence or instrumentalities of crime commonly requires the seizure of the entire computer's input/output periphery devices (including related documentation, passwords and security devices) so that a qualified expert can accurately retrieve

the system's data in a controlled environment.

26. The computer and its storage devices, the mouse, the monitor, keyboard, printer, modem and other system components are also used as instrumentalities of the crime to operate the computer to commit offenses involving the sexual exploitation of minors. Devices such as modems and routers can contain information about dates, IP addresses, MAC addresses, frequency, and computer(s) used to access the Internet or to otherwise commit the crimes described herein. The computer equipment may also have fingerprints on them indicating the user of the computer and its components.

27. Information or files related to the crimes described herein are often obtained from the Internet or the cellular data networks using application software which often leaves files, logs or file remnants which would tend to show the identity of the person engaging in the conduct as well as the method of location or creation of the images, search terms used, exchange, transfer, distribution, possession or origin of the files. Files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

28. "User attribution" evidence can also be found on a computer and is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books,

"chat," instant messaging logs, photographs, videos, and correspondence (and the data associated with the foregoing, such as file creation and last accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time. For example, I know from training and experience that persons trading in, receiving, transporting, distributing or possessing images involving the sexual exploitation of children or those interested in the firsthand sexual exploitation of children often communicate with others through correspondence or other documents which could tend to identify the origin and possessor of the images as well as provide evidence of a person's interest in child pornography or child sexual exploitation. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

29. I know from training and experience that digital software or hardware exists that allows persons to share digital access over wired or wireless networks allowing multiple persons to appear on the Internet from the same IP address. Examination of these items can reveal information about the authorized or unauthorized use of Internet connection at the residence.

30. Searching computer(s) for the evidence described in the attachment may require a range of data analysis techniques. For example, information regarding user attribution or Internet use is located in various operating system log files that are not easily located or reviewed. Or, a person engaged in criminal activity will attempt to conceal evidence of the activity by "hiding" files or giving them deceptive names. As explained above, because the warrant calls for records of how a computer has been used, what it has been used for, and who

has used it, it is exceedingly likely that it will be necessary to thoroughly search storage media to obtain evidence, including evidence that is not neatly organized into files or documents. Just as a search of a premises for physical objects requires searching the entire premises for those objects that are described by a warrant, a search of this premises for the things described in this warrant will likely require a search among the data stored in storage media for the things (including electronic data) called for by this warrant. Additionally, it is possible that files have been deleted or edited, but that remnants of older versions are in unallocated space or slack space. This, too, makes it exceedingly likely that in this case it will be necessary to use a multitude of techniques, both on and off-scene, including more thorough techniques.

31. Furthermore, because there is probable cause to believe that the computer and its storage devices are all instrumentalities of crimes involving child exploitation, they should all be seized as such.

32. Based upon my knowledge, training, and experience, I know that a thorough search for information stored in digital storage media requires a variety of techniques, that often includes both on-site seizure and search as well as a more thorough review off-site review in a controlled environment. This variety of techniques is required, and often agents must seize most or all storage media to be searched on-scene and/or later in a controlled environment. These techniques are often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction.

33. For example, the search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following on-site

techniques (the following is a non-exclusive list, as other on-site search procedures may be used):

A) On-site triage of computer systems to determine what, if any, peripheral devices or digital storage units have been connected to such computer systems, a preliminary scan of image files contained on such systems and digital storage devices to help identify any other relevant evidence or potential victims, and a scan for encryption software;

B) On-site copying and analysis of volatile memory, which is usually lost if a computer is powered down, and may contain information about how the computer is being used, by whom, when, and may contain information about encryption, virtual machine software (virtual operating systems that are lost if the computer is powered down or encrypted);

C) On-site forensic imaging of any computers may be necessary for computers or devices that may be partially or fully encrypted, in order to preserve unencrypted electronic data that may, if not immediately imaged on-scene, become encrypted and accordingly unavailable for any examination.

34. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include off-site techniques since it is often necessary that some computer equipment, peripherals, instructions, and software be seized and examined off-site and in a controlled environment. This is true because of the following:

D) The nature of evidence. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of

how, when and why a computer has been used, by whom, what it has been used for, requires considerable time, and taking that much time on premises could be unreasonable. Also, because computer evidence is extremely vulnerable to tampering and destruction (both from external sources and from code embedded in the system as a "booby-trap"), the controlled environment of a laboratory may be essential to its complete and accurate analysis. Searching for and attempting to recover any deleted, hidden, or encrypted data may be required to determine whether data falls within the list of items to be seized as set forth herein (for example, data that is encrypted and unreadable may not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of child exploitation offenses).

E) The volume of evidence and time required for an examination. Storage media can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files are evidence or instrumentalities of crime. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence.

Reviewing information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

F) Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on-site. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

G) Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

H) Need to review evidence over time and to maintain entirety of evidence. I recognize the prudence requisite in reviewing and preserving in its original form only such records applicable to the violations of law described in this Affidavit and in Attachment B in order to prevent unnecessary invasion of privacy and overbroad searches. I advise it would be impractical and infeasible for the Government to review the mirrored images of digital devices that are copied as a result of a search warrant issued pursuant to this Application during a single

analysis. I have learned through practical experience that various pieces of evidence retrieved from digital devices in investigations of this sort often have unknown probative value and linkage to other pieces of evidence in the investigation until they are considered within the fluid, active, and ongoing investigation of the whole as it develops. In other words, the weight of each individual piece of the data fluctuates based upon additional investigative measures undertaken, other documents under review and incorporation of evidence into a consolidated whole. Analysis is content-relational, and the importance of any associated data may grow whenever further analysis is performed. The full scope and meaning of the whole of the data is lost if each piece is observed individually, and not in sum. Due to the interrelation and correlation between pieces of an investigation as that investigation continues, looking at one piece of information may lose its full evidentiary value if it is related to another piece of information, yet its complement is not preserved along with the original. In the past, I have reviewed activity and data on digital devices pursuant to search warrants in the course of ongoing criminal investigations. I have learned from that experience, as well as other investigative efforts, that multiple reviews of the data at different times is necessary to understand the full value of the information contained therein, and to determine whether it is within the scope of the items sought in Attachment B. In order to obtain the full picture and meaning of the data from the information sought in Attachments A and B of this application, the Government would need to maintain access to all of the

resultant data, as the completeness and potential of probative value of the data must be assessed within the full scope of the investigation. As such, I respectfully request the ability to maintain the whole of the data obtained as a result of the search warrant, and to maintain and to review the data in the control and custody of the Government and law enforcement at times deemed necessary during the investigation, rather than minimize the content to certain communications deemed important at one time. As with all evidence, the Government will maintain the evidence and mirror images of the evidence in its custody and control, without alteration, amendment, or access by persons unrelated to the investigation.

35. Based on the foregoing, and consistent with Rule 41(e)(2)(B), when persons executing the warrant conclude that it would be impractical to review the media on-site, the warrant I am applying for permits both on-site seizing, imaging and searching as well as off-site imaging and searching of storage media that reasonably appear to contain some or all of the evidence described in the warrant, thus permitting its later and perhaps repeated examination consistent with the warrant. The examination may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

36. Because several people may share the SUBJECT PROPERTY as a residence, it is possible that the SUBJECT PROPERTY will contain computers that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

37. I know from training and experience that digital storage devices can be very large in capacity, yet very small in physical size. Additionally, I know from training and experience that those who are in possession of such devices also tend to keep them on their persons, especially when they may contain contraband or other evidence of a crime. The storage capacity of such devices can be as large as tens of gigabytes in size as further described below, which allows for the storage of thousands of images and videos as well as other digital information such as calendars, contact lists, programs and text documents. Such storage devices can be smaller than a postage stamp in size, which allows them to be easily hidden in a person's pocket.

BACKGROUND REGARDING THE INTERNET AND CHILD EXPLOITATION

38. I have education and training in information technology and its use in criminal activities. I own my own computer, have personal knowledge of the operation of a computer, and have accessed the Internet for numerous years. Based on this training and knowledge, and the experience of other law enforcement personnel involved in this investigation, I know the following:

39. Child pornographers can produce images using a wireless device such as a cell phone. Photos can also be made using cameras, then can be transferred onto another device either using wire or wireless technology. Images can also be uploaded to Internet-based storage commonly referred to as the "cloud." Hard-copy images can also be scanned into a computer. Via the Internet, connection can be made to literally millions of computers around the world. Child pornography can be transferred quickly and easily via electronic mail or virtually countless other online platforms, communication services, storage services, and applications.

40. A computer's capability to store images in digital form makes it an ideal repository

for child pornography and other files related to the sexual abuse and exploitation of children. The digital-storage capacity in devices and in the "cloud" has grown tremendously within the last several years. Thumb drives with a capacity of 128 GB are not uncommon. Flash cards with a capacity of 64 gigabytes are not uncommon. Hard drives with the capacity of 500 gigabytes up to 3 terabytes are not uncommon. Phones with over 100 gigabytes in storage are not uncommon. Devices can store thousands of images and videos at very high resolution. These devices are often internet capable and can not only store but can transmit images via the internet and can use the devices to store images and documents in internet or "cloud" storage spaces. Once this is done, there is no readily apparent evidence at the "scene of the crime". Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

41. With Internet access, a computer user can transport an image file from the Internet or from another user's computer to his own computer, so that the image file is stored in his computer. The process of transporting an image file to one's own computer is called "downloading". The user can then display the image file on his computer screen and can choose to "save" the image on his computer and/or print out a hard copy of the image by using a printer device (such as a laser or inkjet printer). Sometimes the only method to recreate the evidence trail of this behavior is with careful laboratory examination of the computer, modem, printer, and other electronic devices.

42. I know from training and experience that search warrants of residences involved in computer or digitally related criminal activity usually produce items that tend to establish ownership or use of digital devices and ownership or use of any Internet service accounts accessed to obtain child pornography to include credit card bills, telephone bills, correspondence and other

identification documents.

43. I know from training and experience that search warrants of residences usually reveal items that tend to show dominion and control of the property searched, to include utility bills, telephone bills, correspondence, rental agreements and other identification documents.

USE OF BIOMETRICS TO UNLOCK DEVICES

44. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, along with information found in publicly available materials published by device manufacturers, many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features rather than with passwords or passcodes. In light of the foregoing circumstances, during the execution of the search of the SUBJECT PREMISES described in **Attachment A**, when attempting to unlock a telephone, computer, or other electronic device whose seizure and search are authorized by this warrant, I am seeking specific authorization for law enforcement personnel to compel the use of an individual's biometric features, if (1) the procedure is carried out with dispatch and in the immediate vicinity of the SUBJECT PREMISES and, if at the time of compulsion, law enforcement personnel has (2) reasonable suspicion that the individual has committed a criminal act that is the subject matter of the warrant, and (3) reasonable suspicion that the individual's biometric features will unlock the device, i.e., there is reasonable suspicion to believe that the individual is the user of the device. Compulsion of an individual's biometric features includes pressing fingers (including thumbs) against and/or putting a face before the sensor, or any other security feature requiring biometric recognition.[1]

[1] *See Matter of Search of [Redacted] WA, DC*, 317 F.Supp. 3d 523, 527-539 (D.D.C. 2018)(comprehensive analysis and ruling that compulsion of biometric features, as requested in this warrant, violates neither the Fourth

45. I respectfully request that the attached warrant be issued authorizing the search of items listed in Attachment A and the seizure of items listed in Attachment B.

Curtis Cox
Special Agent
Federal Bureau of Investigation

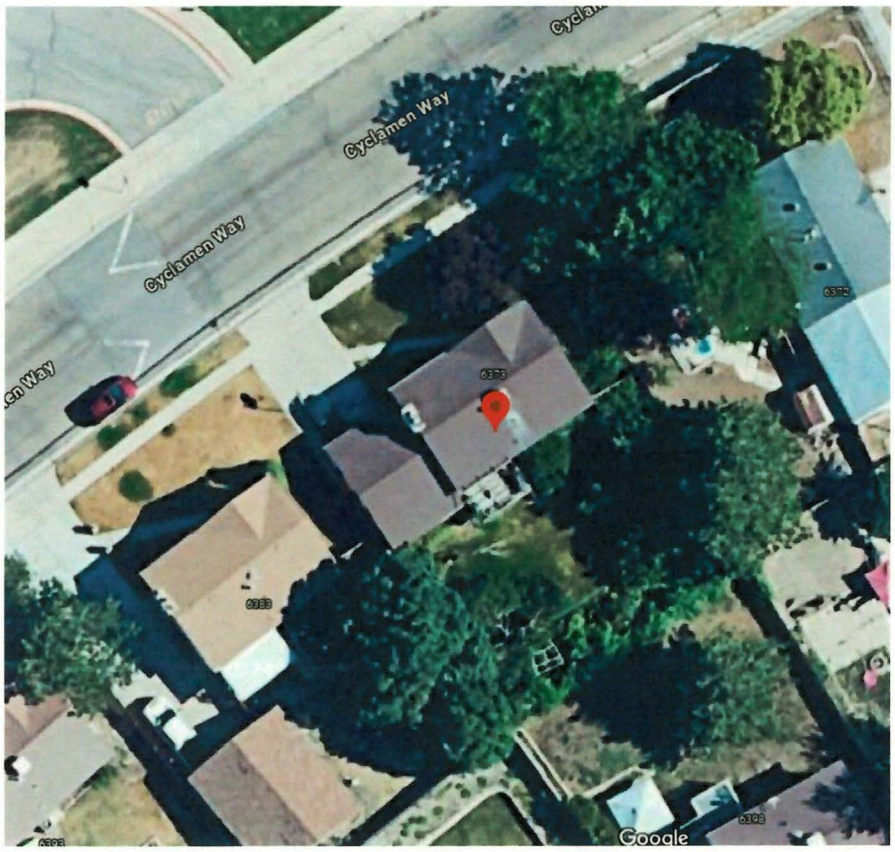
Sworn and subscribed before me this 10 day of October, 2024.

Daphne A. Oberg
United States Magistrate Judge

Amendment's requirements nor the Fifth Amendment's self-incrimination clause); *In the Matter of the Search of: a White Google Pixel 3 XL Cellphone in a Black Incipio Case*, 398 F.Supp. 3d 785, 789-94 (D. Idaho 2019)(compulsion of biometric features non-testimonial and therefore not violative of suspect's Fifth Amendment right); *In the Matter of the Search of the Search Warrant Application for the Cellular Telephone in United States v. Barrera*, 415 F.Supp. 3d 832, 835-42 (N.D. Ill. 2019)(compulsion of biometric features non-testimonial); *In re Search Warrant No. 5165*, ___ F. Supp. 3d ___, 2020 WL 3581608 (E.D. Ky. 7/2/2020)(adopting and applying D.C. District Court's above decision in striking a warrant's request to compel biometric features from "all individuals" at the premises during the search as overbroad); *but see United States v. Wright*, 431 F. Supp. 3d 1175, 1185-88 (D. Nev. 2020)(unlocking phone with defendant's facial features is testimonial and a violation of Fifth Amendment right); *In the Matter of the Search of a Residence in Oakland, California*, 354 F. Supp. 3d 1010, 1015-16 (N.D. CA 2019)(utilizing biometric feature to unlock phone is testimonial).

ATTACHMENT A
PREMISES TO BE SEARCHED

The property to be searched (SUBJECT PROPERTY) is the property located at 6373 South Cyclamen Way, West Jordan, Utah. The SUBJECT PROPERTY contains a home that appears to be a single family, split-level residence. The home is yellow in color, with a reddish front door, brown roof and trim, and a brick façade on the bottom front portion of the home. On the single step leading to the front door, the number "6373" is painted in black on a white background. The front door is accessible from Cyclamen Way. The SUBJECT PROPERTY includes the entire property, including any outbuildings, sheds, garages, vehicles, and RVs that may be located on the property.


Cyclamen Way
Cyclamen Way
Google

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED AND SEARCHED

The following items to be seized constitute fruits, instrumentalities, and evidence of violations of 18 U.S.C. §§ 2252(a)(4), 2252A(a)(2), and (5)(B) (Receipt, Possession, and Access to View Child Pornography) (the "SUBJECT OFFENSES"):

1. Images or visual depictions of child pornography.

2. Records and information containing child erotica, including texts, images, and visual depictions of child erotica.

3. Any and all information, notes, software, documents, records, or correspondence, in any format and medium, pertaining to violations of the SUBJECT OFFENSES:

4. Any and all information, notes, documents, records, or correspondence, in any format or medium, concerning communications about child pornography or sexual activity with or sexual interest in minors.

5. Any and all information, notes, documents, records, or correspondence, in any format or medium, concerning Internet activity reflecting a sexual interest in minors or child pornography.

6. Any and all information, notes, software, documents, records, or correspondence, in any form and medium pertaining to any minor who is, or appears to be, the subject of any visual depiction of child pornography, child erotica, sexual activity with other minors or adults, or of sexual interest, or that may be helpful in identifying any such minors.

7. Any and all address books, names, and lists of names and addresses of individuals who may have been contacted by user of the computer or by other means for the purpose of committing violations of SUBJECT OFFENSES.

8. Any and all information, notes, documents, records, or correspondence, in any format or medium, concerning membership in online groups, clubs, or services that provide or make accessible child pornography.

9. Any and all cameras, film, videotapes or other photographic equipment that constitute evidence of the commission of, contraband, the fruits of crime, or instrumentalities of violations of the SUBJECT OFFENSES.

10. Any and all information, records, documents, invoices and materials, in any format or medium, that concern any accounts with an Internet Service Provider pertaining to violations of the SUBJECT OFFENSES.

11. Any and all information, records, documents, invoices and materials, in any format or medium, that concern e-mail accounts, online storage, or other remote computer storage pertaining to violations of the SUBJECT OFFENSES.

12. Any and all information, documents, records, photos, videos, or correspondence, in any format or medium, pertaining to occupancy or ownership of the premises and use or ownership of computer equipment found in the premises, or that aid in the identification of persons involved in violations of the SUBJECT OFFENSES.

13. Credit cards, credit card information, bills and payment records pertaining to violations of the SUBJECT OFFENSES.

14. Information about usernames or any online accounts or email addresses or Internet Service Providers used in the commission of violations of the SUBJECT OFFENSES.

15. Computer(s), digital storage media, or digital storage devices, any physical object upon which computer data can be recorded, computer hardware, computer software, servers, computer related documentation, computer passwords and data security devices, gaming devices, tablets, flash drives, volatile data, digital communications devices, cellular telephones, cameras, videotapes, video recording devices, video recording players, and video display monitors, digital input and output devices such as keyboards, mouse(s), scanners, printers, monitors, electronic media and network equipment, modems, routers, connection and power cords, and external or connected devices used for accessing computer storage media that was used to commit or facilitate commissions of the SUBJECT OFFENSES.

16. For any computer, computer hard drive, or other physical object upon which computer data can be recorded (hereinafter, COMPUTER) that is called for by this warrant, or that might contain items otherwise called for by this warrant:

    a. evidence of who used, owned, or controlled the COMPUTER at the time the items described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, calendars, browsing history, user profiles, e-mail, e-mail contacts, "chat" or instant messaging logs, photographs, and correspondence;

    b. evidence of software that may allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

    c. evidence of the lack of such malicious software;

    d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

    e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. evidence of how and when the COMPUTER was used or accessed to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

g. records of or information about Internet Protocol addresses used by the COMPUTER;

h. evidence indicating the computer user's state of mind as it relates to the crime under investigation, namely crimes involving child exploitation and child pornography;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. contextual information necessary to understand the evidence described in this attachment;

l. volatile data necessary to preserve evidence prior to powering-off and unplugging a running computer.

m. images and visual depictions of child pornography;

n. records and information containing child erotica, including texts, images and visual depictions of child erotica;

o. any and all information, notes, software, documents, records, or correspondence, in any format and medium, pertaining to violations of 18 U.S.C. §§ 2252(a)(1), (2), and (4) and 2252A(a)(1), (2), (3), and (5);

p. any and all information, notes, documents, records, or correspondence, in any format or medium, concerning communications about child pornography or sexual activity with or sexual interest in minors;

q. items otherwise described above in paragraphs 1- 14 of this Attachment B;

r. when attempting to unlock a telephone, computer, or other electronic device identified above, whose seizure and search are authorized by this warrant, law enforcement personnel may compel the use of an individual's biometric features, if: (1) the procedure is carried out with dispatch and in the immediate vicinity of the SUBJECT PREMISES and, if at the time of compulsion, law enforcement personnel has (2) reasonable suspicion that the individual has committed a criminal act that is the subject matter of the warrant, and (3) reasonable suspicion that the individual's biometric features will unlock the device, i.e., there is reasonable suspicion to believe that the individual is the user of the device. Compulsion of an individual's biometric features includes pressing fingers (including thumbs) against and/or putting a face

before the sensor, or any other security feature requiring biometric recognition. This does not authorize law enforcement personnel to compel disclosure of a password, swipe pattern, or other non-biometric/physical login.

DEFINITIONS:

17. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

18. "Child Pornography" is defined in 18 U.S.C. § 2256(8), which includes as any visual depiction of sexually explicit conduct involving the use of a minor; a digital image, computer image, or computer-generated image that is, or is indistinguishable from that of a minor engaged in sexually explicit conduct; or a visual depiction that has been created, adapted, or modified to appear than an identifiable minor is engaging in sexually explicit conduct.

19. "Visual depiction" includes prints, copies of visual images, developed and undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

20. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions; this also includes texts or discussions regarding minors engaged in sexual acts or conduct.

As used above, the terms "computers" or "digital storage media" or "digital storage devices" may be used interchangeably, and are intended to include any physical object upon which computer data can be recorded as well as all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices capable of performing logical, arithmetic, or storage functions, including desktop and laptop computers, mobile phones, tablets, server computers, game consoles, network hardware, hard disk drives, RAM, floppy disks, flash memory, CDs, DVDs, and other magnetic or optical storage media